I-CLICK SECURITY TIPS

1. Accessing I-Click

- Always access I-click by typing URL https://www.imbank.com and then going to Internet Banking link.
- Never click on a link in an email to take you to a website and enter personal details either in the email or website.
- Whenever possible avoid login to I-click on public computers or cyber cafes. If it is urgent and you find yourself doing it, change your password immediately you get your home computer.
- Note that some Wi-Fi connections are just like cyber cafes. So do not access I-click services from an open unsecure Wi-Fi hotspot. If you do not know the business responsible for maintaining the Wi-Fi hotspot, do not access Internet banking services from it. Access Internet banking services only from a Wi-Fi hotspot maintained by reputable organizations.
- It is good cyber security practice to use the Virtual Keyboard (onscreen) when logging in to I-click.

2. Password Security

- You should always be cautious if you receive unsolicited emails or calls asking you to disclose any personal details such as internet banking user names and passwords, bank account numbers or bank registered phone numbers. This information should be kept secret at all times.
- Never disclose personal information to individuals you do not know. I&M Bank would never contact you to ask you to disclose your internet banking user names and passwords, bank account numbers or bank registered phone numbers.
- Never write down or store your passwords in a file on your computer.
- Don't share your username and password with others. Be cautious of sharing your usernames and passwords with sites, software, or services- especially when your personal information and money is involved.
- Never use online password storage.
- Make your password lengthy. Your password should be 8 characters or more and a combination of alphabets and numbers. Don’t use a password that is easy to guess e.g. family name.
- Where possible, use passphrases which include a long sentence of a familiar phrase to you e.g. the chorus of a song or a phrase in a poem.

3. Ensure I-click session is secure

When undertaking any banking on I-click, check that the session is secure.
There are two simple indicators that will tell you if your session is secure.

- The first is the presence of https:// in the URL (address box) e.g. https://netbanking.imbank.com Some browsers such as Mozilla Firefox change the colour of the URL window when you are in a secure session.
- The other indicator is the presence of a digital certificate represented by a padlock or key in the bottom right hand corner. If you double click on this icon it should provide you with information about the organization with which you have entered in to a secure session.

4. Computer Security

- It is important to use up-to-date Anti-virus software. If your computer uses Microsoft Windows operating system, it is important to keep it updated via the Windows Update feature, equally if you use another PC operating system or have an Apple Mac you should check regularly for updates.
- You should be vigilant if you use Internet cafes or a computer that is not your own and over which you have no control.
- In addition to being protected by using up-to-date antivirus software you should also regularly use software to remove Spyware from your computer, as these programs record information about your Internet use and transmit it without your permission. In some circumstances this can compromise your PC security.
- Avoid downloading files from unknown sources. Malicious software (also known as 'malware') and computer viruses can be hidden in email attachments and other files downloaded from the Internet. Before you download anything, verify you trust the source. Even when you receive files from friends and family, make sure your anti-virus software scans the files before opening them.

5. I-Click Log-off

It is important to completely log off from your Internet banking session; simply closing the window you performed the transaction in may not close the banking session. If your computer is infected with a Trojan virus, you session may become hijacked by a criminal and financial transactions performed without your knowledge. It is also advisable to disconnect from the Internet if you are not planning to use it.

Make sure that you see the message below from i-click confirming successful log-off

6. Email and website tricks

Fraudsters send out fake emails to random email addresses hoping to reach real unsuspecting customers.
These emails are called 'phishing' emails. Never respond to an email if you don't know the sender.

Fraudsters create fake websites that look like real company websites in order to steal your personal information.
Always access Iclick from https://www.imbank.com

Social networks such as Facebook, Twitter, LinkedIn and MySpace allow you to share your information online.
Never share your banking information on social sites, whether account related or Debit/Credit Card related.
Also, do not give too much information unknowingly, including where you Bank or even the specific branch you carry out your banking from.

7. Check your statements

It is important to check your statements regularly; a quick check will help identify any erroneous or criminal transactions that might have been performed on your account without your knowledge.

8. Bank Hotlines

In case you doubt any request for information (email,telephone,sms,pop-ups etc.) or you become suspicious of an activity that threatens your account security, contact the Bank immediately on iclicksupport@imbank.co.ke or call (+254)-020-322100 for assistance.